Department of Justice
California Justice Information Services Division
Conditions for Release of Criminal Offender Record Information

Criminal offender record information (CORI) may be released to public agencies or bona fide research bodies provided that the data is used only for research and statistical purposes pursuant to California Penal Code (PC) section 13202 and subject to the conditions listed below. CORI is defined in PC section 11077 as records and data compiled by criminal justice agencies for the purpose of identifying criminal offenders and for maintaining a summary of arrests, pretrial proceedings, the nature and disposition of criminal charges, sentencing, incarceration, rehabilitation, and release. The California Department of Justice (DOJ) database which contains CORI is the Automated Criminal History System.

1. Requests must be in writing and must specify the intended use for the data. All research requests must be accompanied by a written request to produce copies of any records as specified in condition #5, and by a security plan as specified in condition #6.

2. When CORI is to be obtained by a law enforcement or criminal justice agency via the California Law Enforcement Telecommunications System for a research project, access shall be by authorized agency staff during low traffic hours.

3. The public agency or bona fide research body receiving CORI is responsible for the care and security of the records. The public agency or bona fide research body receiving CORI will not receive personal identifiers such as name of subject, Federal Bureau of Investigation (FBI) number, State Identification (SID) number, social security number, driver's license number and California Department of Corrections (CDC) number unless there is a demonstrated compelling need for this information. The need for personal identifying information shall be in writing and will be reviewed on a case by case basis.

4. All staff members from any public agency or bona fide research body who have direct or indirect access to CORI provided by the DOJ for research must complete a fingerprint background check and are required to sign the Researcher Security and Disclosure Form provided by the DOJ; including but not limited to research staff, IT staff, and system administrators.

5. The public agency or bona fide research body receiving CORI is strictly prohibited from using the data for any purpose other than the purpose for which the data was provided. The public agency or bona fide research body shall not produce copies of CORI provided by the DOJ unless specified in the data security plan. CORI obtained from the DOJ is confidential and, under penalty of law (PC section 11142), may not be disseminated to a third party.

6. The public agency or bona fide research body must take reasonable precautions to protect CORI from unauthorized access. The public agency or bona fide research body is required to submit to the DOJ a detailed plan of the security measures in place to guard against unauthorized access of hard copies or electronic files containing CORI. Please refer to the attached Criminal Offender Record Information Data Security Checklist document for additional information and guidelines regarding the security of CORI.

7. It is incumbent upon the public agency or bona fide research body to prevent disclosure of CORI from unauthorized users throughout the duration of the research project and to immediately report any security breach to the DOJ.

8. The public agency or bona fide research body receiving CORI must destroy the CORI in accordance with the FBI CJIS Security Policy version 5.6:

5.8.3 Digital Media Sanitization and Disposal

The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

5.8.4 Disposal of Physical Media

Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

The DOJ must be notified in writing (for address, see condition #10) confirming the destruction of electronic and/or hard copy records.

9. Periodic unannounced site inspections and scheduled audits may be performed by the DOJ to ensure compliance with the DOJ's policies and regulations.

10. When data derived from criminal offender record information records is used or referenced in any publication, a copy of that publication must be furnished to:

California Department of Justice
California Justice Information Services Division
Research Center
PO Box 903417, Room G-110
Sacramento, CA 94203-4170
researchrequest@doj.ca.gov

11. A public agency or bona fide research body is required to notify the DOJ when a team member is added or removed from the research project.

12. The public agency or bona fide research body is required to notify the DOJ once the project has been completed.

I have read and understand the preceding Conditions for Release of Criminal Offender Record Information. I understand that failure to comply with these conditions may result in the loss of access to criminal offender record information for this and/or future research projects, and that the DOJ reserves the right to revise these conditions, or impose additional conditions, at any time it deems necessary to protect the confidentiality and security of information maintained by the DOJ.

Signature

Date

Printed Name

Position

Name of Public Agency/Research Organization